

A B S T R A C T

A METHOD AND APPARATUS FOR ANONYMOUS SIGNATURE BY MEANS
OF A SHARED PRIVATE KEY

5 The invention concerns a cryptographic method and
apparatus for anonymously signing a message. The method
consists in adding to the anonymous signature an
additional signature which is calculated (operation 13)
10 using a private key common to all the members of a group
authorized to sign and unknown to all revoked members.
Said private key is updated (operations 8, 11) at group
level on each revocation within the group and at member
level only on anonymous signing of a message by the
15 member. The apparatus comprises as many smart cards as
there are members in the group and apparatus comprising
first calculating means.

20

25

30

35 Translation of the title and the abstract as published by the PCT Authorities,
possibly after making changes, ex officio, e.g. under PCT Rules 37.2, 38.2, and/or
48.3.